AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently Amended): An authentication system comprising a server system communicably connected to a communication terminal via a communication network, wherein a user handles the communication terminal to access data stored in the server system via the communication network, the server system comprising:

a first authentication unit configured to receive user-identifying information from the communication terminal via the communication network, authenticate the user-identifying information, and generate first key information based on the authenticated user-identifying information, the first key information being transmitted to the user;

a second authentication unit configured to receive the first key information from the communication terminal via the communication network, ~~to~~ authenticate the first key information every time the first key information is received, and generate new second key information based on the same first key information every time the first key information is received, the new second key information generated each time entitling the user to ~~repeatedly~~ access the data in the server system for a specified period of time as long as the communication terminal is activated, ~~and~~ the second key information being transmitted to the communication terminal via the communication network; and

an access permitting unit configured to receive the second key information from the communication terminal via the communication network and permit the user to access the data in the server system for the specified period of time every time the user accesses the server system.

Claim 2 (Previously Presented): The authentication system according to claim 1, further comprising a second server system which is connected to the communication network and different from the server system generating the second key information,

wherein the second server system comprises a third authentication unit configured to authenticate validity of the second key information.

Claim 3 (Previously Presented): The authentication system according to claim 2, wherein the second server system is configured to set a period of time to permit the user to access the data on the basis of both of a time instant at which the second key information is generated and a time remaining in the specified period of time set for the access to be carried out using the second key information.

Claim 4 (Currently Amended): A server system for use in an authentication system and which is communicably connected with a communication terminal via a communication network, wherein a user handles the communication terminal to access data stored in the server system via the communication network, the server system comprising:

a first authentication unit configured to receive user-identifying information from the communication terminal via the communication network, authenticate the user-identifying information, and generate first key information based on the authenticated user-identifying information, the first key information being transmitted to the user;

a second authentication unit configured to receive the first key information from the communication terminal via the communication network, authenticate the first key information every time the first key information is received, and generate new second key information based on the same first key information every time the first key information is received, the new second key information generated each time entitling the user to ~~repeatedly~~ access the data in the server system for a specified period of time as long as the communication terminal is activated and the second key information being transmitted to the communication terminal via the communication network; and

an access permitting unit configured to receive the second key information from the communication terminal via the communication network and permit the user to access the data in the server system for the specified period of time every time the user accesses the server system.

Claim 5 (Previously Presented): The server system according to claim 4, wherein the first key information is an access key for accessing the server system to acquire the second key information and the second key is a session key for accessing the data in the server system and requesting transmission of the data.

Claim 6 (Previously Presented): The server system according to claim 4, in cases where the user-identifying information is transmitted using a second communication terminal other than the communication terminal handled by the user, the first authentication unit transmits, to the second communication terminal, a second access key generated based on the user-identifying information provided from the second communication terminal, the second access key being regarded as being the same as the previously-generated access key.

Claim 7 (Previously Presented): The server system according to claim 4, wherein the communication terminal is configured to provide terminal-identifying information to the server system together with the user-identifying information, wherein the terminal-identifying information is used for the authentication by the first authentication unit.

Claim 8 (Currently Amended): An authentication method carried out by a server system communicably connected to a communication terminal via a communication network, wherein a user handles the communication terminal to have access to data stored in the server system via the communication network, the method comprising:

receiving user-identifying information transmitted from the communication terminal via the communication network;

authenticating the received user-identifying information;

generating, only once, first key information based on the authenticated user-identifying information;

transmitting the first key information to the communication terminal;

receiving the first key information from the communication terminal via the communication network;

authenticating the received first key information every time the first key information is received;

generating new second key information based on the same first key information every time the first key information is received, the new second key information generated each time entitling the user to periodically access the data in the server system for a specified period of time as long as the communication terminal is activated;

transmitting the second key information to the communication terminal via the communication network;

receiving the second key information from the communication terminal via the communication network; and

permitting the user to access the data in the server system for the specified period of time every time the user accesses the server system.

Claim 9 (Previously Presented): The authentication method according to claim 8, wherein the first key information is an access key for accessing the server system to acquire the second key information and the second key is a session key for accessing the data in the server system and requesting transmission of the data.

Claim 10 (Canceled).

Claim 11 (Previously Presented): The authentication method according to claim 8, wherein the communication terminal provides terminal-identifying information to the server system together with the user-identifying information, wherein the authenticating of the user-identifying information uses the terminal-identifying information.

Claim 12 (Previously Presented): The authentication method according to claim 8, further comprising authenticating validity of the second key information.

Claim 13 (Previously Presented): The authentication method according to claim 8, wherein the generating of the second-key information includes the step of setting a period of

time to permit the user to access the data in the server system on the basis of both of a time instant at which the second key information is generated and a time remaining in the specified period of time set for the access to be carried out using the second key information.

Claim 14 (Canceled).

Claim 15 (Previously Presented): A computer program product comprising a computer readable medium having computer-readable program code embodied thereon, the program code, when executed, being adapted to carry out the method of claim 8.

Claim 16 (Currently Amended): An authentication method for authenticating a user terminal requesting access to data stored in a server system, the method comprising:

receiving secured user information from a user of the user terminal;

authenticating the received user information;

generating an access key based on the authenticated user information;

transmitting the access key to the user;

receiving the access key from the user terminal via a communication network at a time of a first request for accessing the data stored in the server system;

authenticating the access key received from the user terminal;

generating a session key based on the access key received from the user terminal;

transmitting the session key to the user terminal via the communication network;

receiving the session key from the user terminal via the communication network;

permitting the user terminal to access the data in the server system if the session key is received within some period of time subsequent to the transmitting of the session key to the user terminal via the communication network; and

transmitting <u>new</u> ~~additional~~ session keys to the user terminal via the communication network in response to receiving the same access key from the user terminal via the communication network at times of additional requests for accessing the data stored in the server system subsequent to the time of the first request.

Claim 17 (Previously Presented): The method according to claim 16, wherein the secured user information is not received again at the subsequent times of the additional requests for accessing the data.

Claim 18 (Previously Presented): The method according to claim 16, wherein the secured user information is secured using a secure sockets layer protocol.

Claim 19 (Previously Presented): The method according to claim 16, further comprising:

receiving the same access key from at least one other, different user terminal;

generating a session key based on the access key;

transmitting the session key to the other user terminal via the communication network;

receiving the session key from the other user terminal via the communication network; and

permitting the other user terminal to access the data in the server system if the session key is received within some period of time subsequent to the transmitting of the session key to the other user terminal via the communication network.

Claim 20 (Previously Presented): The method according to claim 16, further comprising:

generating at least one other access key based on the authenticated user information;

transmitting the other access key to at least one other different user terminal;

receiving the access key from the other user terminal via the communication network at a time of a first request for accessing the data stored in the server system;

authenticating the access key received from the other user terminal;

generating a session key based on the access key received from the other user terminal;

transmitting the session key to the other user terminal via the communication network;

receiving the session key from the other user terminal via the communication network; and

permitting the other user terminal to access the data in the server system if the session key is received within some period of time subsequent to the transmitting of the session key to the other user terminal via the communication network.

Claim 21 (Previously Presented): The method according to claim 16, further comprising:

receiving a hardware identifier transmitted from the user terminal over a communication network,

wherein the authenticating is based on both the secured user information and the hardware identifier.